

REMARKS

In response to the corrected Final Office Action mailed January 15, 2008, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks, have canceled claims and have amended claims. The claims as now presented are believed to be in allowable condition.

Claims 17, 32, 37, 38, and 43-52 were pending in this Application. By this Amendment, claims 17, 32, 48, 50, and 51 have been canceled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Accordingly, claims 37-38, 43-47, 49, and 52 are now pending in this Application. Claims 37, 38, 43, 45, and 52 are independent claims.

Rejections under §103

Claims 37, 38, 48 and 50-52 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0226023 (Peters) in view of U.S. Patent No. 6,397,334 (Chainer, et al.). Claims 43-47 and 49 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peters in view of Chainer and further in view of U.S. Patent No. 5,517,568 (Grube, et al.).

Applicants respectfully traverse these rejections and request reconsideration. The claims are in allowable condition.

Peters teaches a technique for deterring theft of media recording devices (Abstract). A media file recorded by a recording device is encrypted, so that it cannot be properly played back without a cryptographic key supplied to the owner of the device (Paragraph 0023). Because asymmetric public key encryption is more secure but also more complex (and therefore slower) than symmetric shared key encryption, a symmetric key may be used to encrypt the media files while the symmetric key is encrypted using public key encryption.

(Paragraph 0031). In order to aid a customer who has lost his or her key to a device, a manufacturer may provide a key escrow service to give a customer the key upon presentation of some proof of ownership of the device (Paragraph 0043).

Chainer discloses a system and method for authenticating an image of an object (Abstract). An object 102 contains one or more tags 101, such as RFID tags, which are not functionally removable from the object 102 (Col. 3, line 63 through Col. 4, line 8). A tag reader 103 (such as an RFID tag reader) reads the RFID tags 101 as a coupled camera system 104 records an image of the object 102 (Col. 4, lines 27-36). A composite generator 105 combines the image and the sensed RFID results to encode the tag ID information together with a hash of the image (Col. 4, lines 37-48). This encoded data may be encrypted for further security (Col. 5, lines 43-54). In addition, other measuring devices 400 may record additional properties of an object 406 in order to provide additional information with which to identify an object (Col. 6, lines 17-38). In addition, a zoom lens 108 may be used to take multiple pictures of an object 102 with different settings (Col. 6, lines 39-45).

Grube discloses a method for detecting unauthorized use of a communication unit 102 in a secure wireless communications system 100 (Col 2, lines 44-45). If a communication unit 102 sends an encrypted communication encrypted with inactive, previously used, encryption parameters (such as a inactive encryption key), then this is detected by system manager 110 (Col. 3, lines 21-36), and the communication unit 102 is flagged as an unauthorized unit (Col. 4, lines 48-60).

#### Claims 43 and 44

Claim 43 (which has now been placed into independent form by incorporating all the limitations previously found in canceled base claim 17)

recites a method for generating an output signal from a video data acquisition system. The method includes (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) implementing a recognition algorithm to identify objects associated with the sensed images, (e) in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal, and (f) randomly generating a new encryption key for encrypting different portions of the video signal over time. Implementing the recognition algorithm to identify objects associated with the sensed images includes analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

The cited references to do not teach or suggest, either alone or in combination, a method including (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) *implementing a recognition algorithm to identify objects associated with the sensed images*, (e) *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal*, and (f) *randomly generating a new encryption key for encrypting different portions of the video signal over time*, in which implementing the recognition algorithm to identify objects associated with the sensed images includes *analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image*.

Peters teaches a technique for deterring theft of media recording devices in which an asymmetric key may be used to encrypt a symmetric key which was used to encrypt video data recorded by a media device. However, Peters does not teach (i) *implementing a recognition algorithm to identify objects associated*

*with the sensed images, (ii) in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal, (iii) randomly generating a new encryption key for encrypting different portions of the video signal over time; and (iv) wherein implementing the recognition algorithm to identify objects associated with the sensed images includes analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.*

The Office Action, on pages 8 and 11, cites Chainer (Figs. 2-3, Col. 4, line 30 through Col. 6, line 17, and Col. 7, lines 52-61) as teaching features (i), (ii), and (iv). However, the cited portion of Chainer does not teach *implementing a recognition algorithm to identify objects associated with the sensed images, and in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal; wherein implementing the recognition algorithm to identify objects associated with the sensed images includes analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.*

Rather, Chainer teaches using an RFID tag reader 103 or other measuring device 400 to record additional data (e.g., a time stamp, focal length, hash of the image, interferometric measurements, biometric data), but not a *recognition algorithm to identify an object from a sensed image*. No image *recognition* is taught in Chainer.

Furthermore, any recognition that may arguably be performed in Chainer does not include *analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image*. The Office Action cited Col. 7, lines 52-61 as teaching this feature. However, although the cited portion notes that the system of that invention could be used to identify people, the cited portion does not teach *analyzing one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image*. Indeed, the cited portion notes "the animate object can be

identified by taking a picture . . . of the animate object while simultaneously obtaining other data (e.g., confirming biometric information such as iris/retinal shape, dental configuration, etc.)" (Col. 7, lines 54-58). Thus, Chainer teaches that while the picture is being taken, biometric information is *simultaneously* obtained separately. Therefore, Chainer does not specifically teach how the identification is effected; it does not teach *analyzing one sensed image to identify a person associated with a pattern depicted in the one sensed image*. This understanding is clarified by the next sentence, which notes that the biometric information could be provided by a tag, such as an RF tag or another device. Therefore, the cited portion merely teaches **somewhat** identifying an animate object, but analyzing a pattern found in a picture is not one of the specified means of identification.

In addition, the additional data of Chainer is merely recorded as a watermark or signature within a recorded image. The additional data may later serve to verify the identity of the recorded image, but in any event, Chainer does not teach *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal* – indeed, any identity verification takes place subsequent to recording the additional data.

The Office Action, on pages 8-9, cites Grube (Col. 1, lines 51-67) as teaching feature (iii). However, the cited portion of Grube does not teach *randomly generating a new encryption key for encrypting different portions of the video signal over time*. Rather, the cited portion of Grube teaches regularly changing the active system encryption parameters (including the encryption algorithm and encryption key) within a secure wireless communication system to maintain security over a long period of time (Col. 1, lines 51-67). However, the cited portion does not teach *randomly* generating a *new* encryption key, nor does it teach using a new encryption key for encrypting *different portions of a video signal over time*. That is, the cited portion could be referring to a pre-provided set of encryption keys that are not *generated* as part of the method. Also, even if the

keys were generated, the cited portion would not teach generating the new keys *randomly* – they could instead be calculated based on a specific pattern. Also, while the cited portion teaches changing the encryption key regularly, it does not teach using the changed keys *for encrypting different portions of a video signal over time* – the cited portion could be limited to encrypting separate signals with different keys and not encrypting one (video or other) signal with multiple keys over time.

Moreover, the Response to Arguments from the Office Action, on pages 2-3, does not respond to the above argument, which was previously presented. In particular, the Office Action does not address Applicants' argument that Grube does not teach *randomly* generating a new encryption key. The Office Action merely cites language indicating that Grube teaches **changing** encryption keys and algorithms over time, but ignores the likelihood that Grube was actually referring to **changing** encryption keys from a pre-provided set of encryption keys that are not *generated* as part of the method. The Office Action Response to Arguments also does not address Applicants' argument that Grube could be limited to encrypting separate signals with different keys and not encrypting one (video or other) signal with multiple keys over time.

Thus, claim 43 patentably distinguishes over Peters in view of Chainer and Grube, and the rejection of claim 43 under 35 U.S.C. §103(a) should be withdrawn.

For the reasons stated above, claim 43 patentably distinguishes over the cited prior art, and the rejection of claim 43 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 43 is now in allowable condition.

Because claim 44 depends from and further limits claim 43, claim 44 is in allowable condition for at least the same reasons. Additionally, it should be understood that dependent claim 44 recites additional features which further patentably distinguish over the cited prior art.

For example, claim 44 recites wherein embedding encrypted data information identifying the recognized object in the output signal includes *encrypting data identifying objects associated with the sensed images with a third key, the third key being distinct from the first key* so that a user, possessing only the third key but not the first key, can decrypt the data identifying objects without having the capability to decrypt the video signal, and including the data encrypted with the third key in the output signal. The Office Action, on page 11, cites Chainer at Col. 4, lines 40-46 as teaching this feature. However, the cited portion does not teach the claimed features. In particular, the cited portion teaches that ID information may be encoded together with other information, such as a time stamp, camera focal length, and a hash of a digital image. While the hash of the digital image may be encrypted (lines 44-45), nowhere does the cited portion indicate that the ID information may be encrypted. The cited portion does use the term "encoded," however, "encoded" is a very broad term that is unlikely to have the meaning "encrypted" in this case. It is very unlikely because in the context it is clear that it means that the ID information is merely **stored** together with the other desired information, concatenated by composite generator 105. Any person having ordinary skill in the art would recognize that "encoded" does not mean "encrypted" in this case. Furthermore, even if, *arguendo*, "encoded" did mean "encrypted" in this case, there is no indication that any encryption was done *with a third key, the third key being distinct from the first key*. Thus, claim 44 further patentably distinguishes over the prior art.

#### **Claims 45 and 46**

Claim 45 (which has now been placed into independent form by incorporating all the limitations previously found in canceled base claim 32) recites an apparatus to support surveillance. The apparatus includes a camera to generate a video signal that varies depending on sensed images. It also includes a memory device to store at least first and second encryption keys and a

processor that encrypts the video signal using the first encryption key. The processor encrypts the first encryption key with the second encryption key and produces an output signal including at least the encrypted video signal and the encrypted first encryption key. The apparatus also includes a recognition system to identify objects associated with the sensed images, the processor embedding encrypted data information identifying the recognized object in the output signal. The apparatus also includes an encryption key generator that randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time. The recognition system analyzes one sensed image of the sensed images to identify a person associated with a pattern depicted in the one sensed image.

The cited references to do not teach or suggest, either alone or in combination, an apparatus having the claimed features. The claimed features are similar to those found in claim 43. Accordingly, claim 45 distinguishes over the prior art for reasons similar to those presented above in connection with claim 43. For the reasons stated above, claim 45 patentably distinguishes over the cited prior art, and the rejection of claim 45 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 45 is now in allowable condition.

Because claim 46 depends from and further limits claim 45, claim 46 is in allowable condition for at least the same reasons. Additionally, it should be understood that dependent claim 46 recites additional features which further patentably distinguish over the cited prior art.

#### **Claims 37 and 47**

Claim 37 (which has now been amended to incorporate limitations previously found in canceled dependent claim 48) patentably distinguishes from the prior art. Claim 37 recites limitations similar to those found in claims 43 and 44. Accordingly, claim 37 distinguishes over the prior art for reasons similar to

those presented above in connection with claims 43 and 44. For the reasons stated above, claim 37 patentably distinguishes over the cited prior art, and the rejection of claim 37 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 37 is now in allowable condition.

Because claim 47 depends from and further limits claim 37, claim 47 is in allowable condition for at least the same reasons. Additionally, it should be understood that dependent claim 47 recites additional features which further patentably distinguish over the cited prior art.

### **Claims 38 and 49**

Claim 38 (which has now been amended to incorporate limitations previously found in canceled dependent claim 50) patentably distinguishes from the prior art. Claim 38 recites limitations similar to those found in claims 43 and 44. Accordingly, claim 38 distinguishes over the prior art for reasons similar to those presented above in connection with claims 43 and 44. For the reasons stated above, claim 38 patentably distinguishes over the cited prior art, and the rejection of claim 38 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 38 is now in allowable condition.

Because claim 49 depends from and further limits claim 38, claim 49 is in allowable condition for at least the same reasons. Additionally, it should be understood that dependent claim 49 recites additional features which further patentably distinguish over the cited prior art.

### **Claim 52**

Claim 52 (which has now been placed into independent form by incorporating all the limitations previously found in canceled base claim 51) patentably distinguishes from the prior art. Claim 52 recites limitations similar to

those found in claims 43 and 44. Accordingly, claim 52 distinguishes over the prior art for reasons similar to those presented above in connection with claims 43 and 44. For the reasons stated above, claim 52 patentably distinguishes over the cited prior art, and the rejection of claim 52 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 52 is now in allowable condition.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Response, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.  
Attorney for Applicants  
Registration No.: 58,203  
Bainwood, Huang & Associates, L.L.C.

-18-

Highpoint Center  
2 Connector Road  
Westborough, Massachusetts 01581  
Telephone: (508) 616-2900  
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-120

Dated: March 17, 2008